# **The Importance of Monitoring on CI/CD, and AWS Services Used Towards It**

The core principle of agile and DevOps is the continuous delivery of value. By architecting and building continuous integration and continuous delivery (CI/CD) pipelines, development teams can automate the process and ensure quality and safety for continuous compliance. CI/CD is at the core of any DevOps practice, combining the processes and tooling that move code changes through the application delivery pipeline. Implementing CI/CD can unlock a competitive advantage for your business, helping you resolve issues faster, reduce time to market, and increase employee and customer satisfaction. Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. **Benefits of CloudWatch**

* Observability on a single platform across applications and infrastructure
* Easiest way to collect metrics in AWS and on-premises
* Improve operational performance and resource optimization
* Get operational visibility and insight
* Derive actionable insights from logs

In addition to Amazon CloudWatch metrics, alarms and dashboards, you can also use a service called [Amazon Managed Service for Grafana (AMG)](https://docs.aws.amazon.com/grafana/latest/userguide/what-is-Amazon-Managed-Service-Grafana.html). Grafana is a widely deployed data visualization tool that is popular for its extensible data support, and AMG is a fully managed and secure data visualization service. You can use AMG to instantly query, correlate, and visualize operational metrics, logs, and traces from multiple sources. AMG makes it easy to deploy, operate, and scale Grafana. Depending on your case or usage, you might already use another service for monitoring and reporting. There are good monitoring and reporting services in the market, and even some open-source services. Make sure to explore every possibility and choose the one that best suits your needs. Remember that the most important part is not which service you use for monitoring: it’s having a way to monitor your systems and be notified about potential issues. As Raf said in one of the videos, operating your infrastructure without monitoring is similar to flying an airplane with no instruments!

# **Preventive and Corrective Actions, Driven by Your Ability to Monitor**

As you learned in this course, monitoring is a key component of DevOps. Monitoring involves collecting metrics and data by automating and instrumentalizing your application’s performance and usage. Because DevOps is a continuous cycle, monitoring isn’t limited to only the deployed production application—you can apply monitoring across the entire DevOps life cycle to further improve your release, deployment, and testing processes. Without monitoring, you wouldn’t be able to track metrics, gather data, analyze the metrics and data for insights, or apply the insights you gain to your application. And with many AWS services, monitoring mechanisms (such as logs, alerts, and the like) are either built into the service itself or provided through other services, like Amazon CloudWatch or AWS CloudTrail.

But what value does monitoring bring to you, as a developer? In business, changes—in the needs of your customers, the market, the business environment, application security, government regulations, and many other areas—are a constant. By using DevOps methodology, you can adapt and even transform your application to address these changes. However, your ability to respond quickly and act proactively to all these changes relies on metrics and data about your application, and the insights you can gain from that data.

As an example, here’s a simple scenario: your team has just deployed a new application to production. Imagine that your team isn’t monitoring the application’s performance or usage. If a problem occurs—say, a server goes down and no failover plan is in place—you might first learn about this issue through customer reports that the support team forwards to you. Before you could take corrective action, you would need to search through multiple sources of information to understand the conditions that resulted in the server failure. And while you are working to resolve the situation, the application remains non-functional, and more customer reports about the application outage continue to come in. Responding to application issues only in a reactive way can be costly in terms of time and resources, and it’s not an ideal situation.

Now, imagine that your team has some basic monitoring mechanisms in place. Though you can use the monitoring tools to correct issues as they occur, monitoring can be used in a preventive way—that is, to prevent issues before they occur. Your team set up some basic instruments to monitor your application servers, such as server utilization metrics, alarms for traffic spikes, different types of logs, and automated notifications to alert you to certain conditions. Adding these instruments helped your application operate more smoothly. You are now alerted when server utilization reaches a critical level (for example, 80%). You can configure the server instances to automatically scale out when a certain utilization threshold is reached, and to scale in when the server utilization decreases to a certain percentage. By monitoring the application and automating how your application responds to monitoring events, you can take preventive action to handle server load before it becomes a problem for your application.

Preventive actions extend to tracking overall application and system health, including data analytics. With monitoring instruments in place, you can capture operational data over a period of time. This data can establish performance baselines for your application, which can surface unusual behavior and other anomalies. Adding a visualization layer to your application’s monitoring data can help you identify trends, gain more insight, and help with troubleshooting your application. If you want to learn more about data analytics on AWS, we also offer another data analytics course on this platform: [Getting Started with Data Analytics on AWS](https://www.coursera.org/learn/getting-started-data-analytics-aws).

As an example, return to previous scenario. The monitoring instruments have been collecting data for a few months, and your team added some visualization tools to help you interpret the data coming in from the logs and metrics. You notice that there’s a cyclical daily increase in application usage that lasts for a couple of hours before it returns to a lower, baseline level. One day, an unusual surge of traffic sets off an alarm notification. You know that the traffic surge is taking place outside of the usual daily peak. Based on the patterns that you see in the visualization dashboard, you suspect that a distributed denial of service (DDoS) event might be taking place, and you can then make sure that your mitigation plan is underway. Your instruments give you visibility into the health of your application, and in turn, you can analyze that data to troubleshoot and optimize your application and continuous integration and continuous delivery (CI/CD) pipelines.

You could further automate the monitoring and operationalizing of your CI/CD pipeline through machine learning (ML). Using ML on monitoring data is a growing trend in DevOps. With ML, you can have an automated way to extract insights from all your monitoring data from all your resources. By doing so, you can identify possible issues, correlate them across multiple services, and remediate them before they cause a problem for your users. A DevOps ML solution could provide more visibility into the operational health of the entire system.

AWS offers an ML service for DevOps. Amazon DevOps Guru is a fully managed service that uses ML to monitor and analyze your operational data in a near-continuous way. Using machine learning models that are informed by years of operational data from Amazon, DevOps Guru produces insights, which are a collection of anomalies (unexpected or unusual metrics) that it identifies during its analysis. Insights can be reactive (reported as they occur) or predictive (reported before the unusual behavior occurs). DevOps Guru also provides recommendations for each insight that suggest how you could improve the performance of your application.

# **The Importance of Operation in CI/CD Pipelines**

Continuous integration and continuous delivery (CI/CD) has become a key component of the software development lifecycle and is the backbone of DevOps. The need for application patching and deployments in monolith and legacy environments are still a reality for multiple enterprises. Sometimes, you might be able to launch new environments, especially if you are working with deployment strategies such as Blue/Green deployment (which is explained in the second course of the series). Sometimes, however, you do not have the ability of create brand new environments, and must work with existing ones. Releasing new features into production by changing a current environment could be challenging because of application complexity, external dependencies, and the coordination of multiple teams in a chain of procedures. [AWS Systems Manager](https://aws.amazon.com/systems-manager/) enables the automation of operational tasks. Systems Manager receives the list of instances to be patched from AWS CodeBuild, and then it remotely runs the commands in all target instances. Systems Manager provides a unified user interface so you can track and resolve operational issues across your AWS applications and resources from a central place. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easier to operate and manage your infrastructure at scale. **Some of its benefits include:**

* Reduces the time needed to resolve operational issues
* Offers easy-to-use automation
* Improves visibility and control
* Manages hybrid environments
* Helps maintain security and compliance
* Connects with IT service management (ITSM) or IT operations management (ITOM) software

Using Run Command, a capability of AWS Systems Manager, you can remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon Elastic Compute Cloud (Amazon EC2) instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Use Run Command to automate common administrative tasks and perform one-time configuration changes at scale. You can use Run Command from the AWS Management Console, the AWS Command Line Interface (AWS CLI), AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

# **AWS Systems Manager**

As you will see in the next segments of the course, AWS Systems Manager is used as a core component on the Operate steps of the DevOps journey. Systems Manager offers many features that facilitate the management of entire fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances and also automations (runbooks) that can be run in the environment.

Stay tuned to learn more about Systems Manager and its capabilities. If you want, you can learn more about it in the following links so that you can be better briefed before watching the videos!

* [AWS Systems Manager – Gain Operational Insights and Take Action (amazon.com)](https://aws.amazon.com/systems-manager/)
* [Introduction to AWS Systems Manager (hands-on.cloud)](https://hands-on.cloud/introduction-to-aws-systems-manager/)
* [Use cases and best practices - AWS Systems Manager (amazon.com)](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-best-practices.html)

Systems Manager can also be used in hybrid environments, where you have servers both running on-premises and in the cloud. First, install the AWS SSM Agent into an operating system (OS) and configure the agent with proper AWS Identity and Access Management (IAM) credentials. After you do so, that OS is identified as a managed OS from the perspective of Systems Manager, and you can use many of the features that Systems Manager provides!

# **Most Common Third-party Services and Tools for DevOps Operations**

Though AWS offers you a suite of services for DevOps operations and monitoring, third-party, open-source tooling is also well known and widely used by the DevOps community.

The following list describes some of the most common open-source DevOps tooling available. In addition, both Puppet and Ansible are members of the AWS Partner Network (APN). There are also many other very good tooling and services for DevOps operations available!

[**Puppet**](http://puppet.com/) Puppet is an infrastructure automation and delivery tool. Puppet is also responsible for publishing one of the most important research papers in the DevOps industry—the famous “State of DevOps” paper, which can be found here: [State of DevOps Report 2021 | Puppet](https://puppet.com/resources/report/2021-state-of-devops-report/).

[**Jenkins**](https://www.jenkins.io/) Jenkins is an open-source automation server. Jenkins provides many plugins to support building, deploying, and automating any project. It’s common to have Jenkins working together with AWS CodePipeline because they developed a [plugin](https://plugins.jenkins.io/aws-codepipeline/) that works with CodePipeline. For more information, see: [Setting up a CI/CD pipeline by integrating Jenkins with AWS CodeBuild and AWS CodeDeploy | AWS DevOps Blog (amazon.com)](https://aws.amazon.com/blogs/devops/setting-up-a-ci-cd-pipeline-by-integrating-jenkins-with-aws-codebuild-and-aws-codedeploy/)

[**Ansible**](https://www.ansible.com/) Ansible, which is sponsored by Red Hat, is also used for IT automation.

Although this course focuses on AWS products and services, being familiar with open-source solutions can be helpful, especially when you need a multi-cloud solution. When you plan your DevOps operations, it’s important to evaluate what AWS solutions and third-party tools make sense as part of your pipeline.